PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : G06F 7/72

A1

(11) International Publication Number: WO 00/39668

(43) International Publication Date: 6 July 2000 (06.07.00)

(21) International Application Number: PCT/CA99/01222

(22) International Filing Date: 23 December 1999 (23.12.99)

(30) Priority Data:
2,257,008 24 December 1998 (24.12.98) CA

(71) Applicant *(for all designated States except US)*: CERTICOM CORP. [CA/CA]; 4th floor, 5520 Explorer Drive, Mississauga, Ontario L4W 5L1 (CA).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: GALLANT, Robert [CA/CA]; 4788 Rosebush Road, Mississauga, Ontario L5M 5N1 (CA). LAMBERT, Robert, J. [CA/CA]; 63 Holm Street, Cambridge, Ontario N3C 3N3 (CA). VANSTONE, Scott, A. [CA/CA]; 10140 Pineview Trail, P.O. Box 490, Campbellville, Ontario L0P 1B0 (CA).

(74) Agents: ORANGE, John, R., S. et al.; Orange Chari Pillay, Toronto Dominion Bank Tower, Suite 3600, Toronto–Dominion Centre, P.O. Box 190, Toronto, Ontario M5K 1H6 (CA).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: A METHOD FOR ACCELERATING CRYPTOGRAPHIC OPERATIONS ON ELLIPTIC CURVES

(57) Abstract

This invention provides a method for accelerating multiplication of an elliptic curve point Q(x,y) by a scalar k, the method comprising the steps of selecting an elliptic curve over a finite field Fq where q is a prime power such that there exists an endomorphism ψ, where $\psi(Q) = \lambda.Q$ for all points Q(x,y) on the elliptic curve; and using smaller representations k_i of the scalar k in combination with the mapping ψ to compute the scalar multiple of the elliptic curve point Q.